§170.315(d)(13) Multi-factor authentication

2015 Edition Cures Update CCG

Version 1.0 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	05-28-2020

Regulation Text

Regulation Text

§ 170.315 (d)(13) *Multi-factor authentication*. Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

(i) Yes – the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "yes," the health IT developer must describe the use cases supported.

(ii) No – the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "no," the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry recognized standards.

Standard(s) Referenced

None

Certification Companion Guide: Multi-factor authentication

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Cures Act Final Rule). It extracts key portions of the ONC Cures Act Final Rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the ONC Cures Act Final Rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition
New	No	Not Included

Technical Explanations and Clarifications

Applies to Entire Criterion

Clarifications:

- The criterion does not require certified health IT to have these capabilities or for health IT developers to implement these capabilities for a specific use case or any use case, just to attest “yes” or “no” to whether the Health IT Module supports multi-factor authentication. The criteria place no requirements on health IT customers, such as health care providers, to implement these capabilities (if present in their products) in their health care settings.

Paragraph (i)

Clarifications:

- If a health IT developer attests “yes” it must describe the use cases supported. For example, a health IT developer could attest “yes” to supporting multi-factor authentication and provide a summary that the Health IT Module supports multi-factor authentication for remote access by clinical users, thus providing clarity on the user roles to which multi-factor authentication applies for that particular Health IT Module.
- Health IT developers are not expected to provide specific technical details about how they support multi-factor authentication as that information could pose security risks. A succinct, high-level summary that gives an indication of the types of uses supported is adequate.
- If a health IT developer adds a new multi-factor authentication use case it must comply with this criterion’s “yes” attestation provisions and be part of the quarterly CHPL reporting by health IT developers and ONC-ACBs under § 170.523(m).

Paragraph (ii)

Clarifications:

- Health IT developers will be permitted, but not required, to provide a reason for attesting “no,” which may be due to multi-factor authentication being inapplicable or inappropriate. In those cases, a health IT developer could, for example, state that the Health IT Module does not support multi-factor authentication because it is engaged in system-to-system public health reporting and multi-factor authentication is not applicable.

Content last reviewed on June 23, 2020